

OCT. 20. 2006 2:50PM  
TO : USPTO

ZILKA-KOTAB, PC

NO. 4447 P. 1

**ZILKA-KOTAB**  
PC  
ZILKA, KOTAB & FEECE™

RECEIVED  
CENTRAL FAX CENTER  
OCT 20 2006

100 PARK CENTER PLAZA, SUITE 300  
SAN JOSE, CA 95113

TELEPHONE (408) 971-2573  
FAX (408) 971-4660

FAX COVER SHEET

Date:	October 20, 2006	Phone Number	Fax Number
To:	Board of Patent Appeals, USPTO	(571) 273-8300	
From:	Kevin J. Zilka		

Docket No.: NAIIP486/01.060.01

App. No: 09/975,991

Total Number of Pages Being Transmitted, Including Cover Sheet: 32

Message:

Please deliver to the Board of Patent Appeals.

Thank you,

Kevin J. Zilka

Original to follow Via Regular Mail  Original will Not be Sent  Original will follow Via Overnight Courier

\*\*\*\*\*  
The information contained in this facsimile message is attorney privileged and confidential information intended only for the use of the individual or entity named above. If the reader of this message is not the intended recipient, you are hereby notified that any dissemination, distribution or copy of this communication is strictly prohibited. If you have received this communication in error, please immediately notify us by telephone (if long distance, please call collect) and return the original message to us at the above address via the U.S. Postal Service. Thank you.  
\*\*\*\*\*

IF YOU DO NOT RECEIVE ALL PAGES OR IF YOU ENCOUNTER  
ANY OTHER DIFFICULTY, PLEASE PHONE Erica  
AT (408) 971-2573 AT YOUR EARLIEST CONVENIENCE

October 20, 2006

Practitioner's Docket No. NAI1P486/01.060.01

**PATENT****IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

In re application of: Neil John Hursey et al.

RECEIVED  
CENTRAL FAX CENTER

Application No.: 09/975,991

Group No.: 2135

Filed: 10/15/2001

Examiner: To, B.

For: MALWARE SCANNING AS LOW PRIORITY TASK

OCT 20 2006

**Mail Stop Appeal Briefs - Patents**  
**Commissioner for Patents**  
**P.O. Box 1450**  
**Alexandria, VA 22313-1450**

**TRANSMITTAL OF APPEAL BRIEF  
(PATENT APPLICATION--37 C.F.R. § 41.37)**

- Transmitted herewith, is the APPEAL BRIEF in this application, with respect to the Notice of Appeal filed on June 12, 2006, and the Notice of Panel Decision from Pre-Appeal Brief Review, mailed 07/20/2006.

**2. STATUS OF APPLICANT**

This application is on behalf of other than a small entity.

**CERTIFICATION UNDER 37 C.F.R. §§ 1.8(a) and 1.10\****(When using Express Mail, the Express Mail label number is mandatory;  
Express Mail certification is optional.)*

I hereby certify that, on the date shown below, this correspondence is being:

**MAILING**

deposited with the United States Postal Service in an envelope addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

**37 C.F.R. § 1.8(a)**

with sufficient postage as first class mail.

**37 C.F.R. § 1.10\***

as "Express Mail Post Office to Addressee"

Mailing Label No. \_\_\_\_\_ (mandatory)

**TRANSMISSION**

✓ facsimile transmitted to the Patent and Trademark Office, (571) 273 - 8300.



Signature

Erica L. Farlow

(type or print name of person certifying)

Date: 10/20/2006

\* Only the date of filing (' 1.6) will be the date used in a patent term adjustment calculation, although the date on any certificate of mailing or transmission under ' 1.8 continues to be taken into account in determining timeliness. See ' 1.703(j). Consider "Express Mail Post Office to Addressee" (' 1.10) or facsimile transmission (' 1.6(d)) for the reply to be accorded the earliest possible filing date for patent term adjustment calculations.

10/23/2006 110111  
 01 FC:1452  
 02 FC:1252  
 500.00 DA  
 450.00 DA  
 00000025 501351  
 69975991

RECEIVED  
CENTRAL FAX CENTER**3. FEE FOR FILING APPEAL BRIEF****OCT 20 2006**

Pursuant to 37 C.F.R. § 41.20(b)(2), the fee for filing the Appeal Brief is:

other than a small entity	\$500.00
<b>Appeal Brief fee due</b>	<b>\$500.00</b>

**4. EXTENSION OF TERM**

The proceedings herein are for a patent application and the provisions of 37 C.F.R. § 1.136 apply.

Applicant petitions for an extension of time under 37 C.F.R. § 1.136 (fees: 37 C.F.R. § 1.17(a)(1)-(5)) for two months:

Fee:	\$450.00
------	----------

If an additional extension of time is required, please consider this a petition therefor.

**5. TOTAL FEE DUE**

The total fee due is:

Appeal brief fee	\$500.00
Extension fee (if any)	\$450.00
<b>TOTAL FEE DUE</b>	<b>\$950.00</b>

**6. FEE PAYMENT**

Authorization is hereby made to charge the amount of \$950.00 to Deposit Account No. 50-1351 (Order No. NAI1P486).

A duplicate of this transmittal is attached.

**7. FEE DEFICIENCY**

If any additional extension and/or fee is required, and if any additional fee for claims is required, charge Deposit Account No. 50-1351 (Order No. NAI1P486).

Reg. No.: 41,429  
Tel. No.: 408-971-2573  
Customer No.: 28875

Signature of Practitioner  
Kevin J. Zilka  
Zilka-Kotab, PC  
P.O. Box 721120  
San Jose, CA 95172-1120  
USA

Transmittal of Appeal Brief--page 2 of 2

- 1 -

**PATENT****IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

In re application of: )  
Hursey et al. ) Group Art Unit: 2135  
Application No. 09/975,991 ) Examiner: To, Baotran N.  
Filed: 10/15/2001 ) Date: 10/20/2006  
For: MALWARE SCANNING AS LOW )  
PRIORITY TASK )  
\_\_\_\_\_  
)

RECEIVED  
CENTRAL FAX CENTER  
OCT 20 2006

Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

**ATTENTION: Board of Patent Appeals and Interferences****APPEAL BRIEF (37 C.F.R. § 41.37)**

This brief is in furtherance of the Notice of Appeal, filed in this case on 06/12/2006.

The fees required under § 1.17, and any required petition for extension of time for filing this brief and fees therefor, are dealt with in the accompanying TRANSMITTAL OF APPEAL BRIEF.

This brief contains these items under the following headings, and in the order set forth below (37 C.F.R. § 41.37(c)(i)):

- I      REAL PARTY IN INTEREST
- II     RELATED APPEALS AND INTERFERENCES
- III    STATUS OF CLAIMS
- IV    STATUS OF AMENDMENTS
- V    SUMMARY OF CLAIMED SUBJECT MATTER
- VI   GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL
- VII   ARGUMENT

- 2 -

- VIII CLAIMS APPENDIX
- IX EVIDENCE APPENDIX
- X RELATED PROCEEDING APPENDIX

RECEIVED  
CENTRAL FAX CENTER  
OCT 20 2006

The final page of this brief bears the practitioner's signature.

OCT. 20. 2006 2:52PM ZILKA-KOTAB, PC

NO. 4447 P. 8

- 3 -

**I REAL PARTY IN INTEREST (37 C.F.R. § 41.37(c)(1)(i))**

The real party in interest in this appeal is McAfee, Inc.

RECEIVED  
CENTRAL FAX CENTER

OCT 20 2006

- 4 -

RECEIVED  
CENTRAL FAX CENTER  
OCT 20 2006

**II RELATED APPEALS AND INTERFERENCES (37 C.F.R. § 41.37(c) (1)(ii))**

With respect to other prior or pending appeals, interferences, or related judicial proceedings that will directly affect, or be directly affected by, or have a bearing on the Board's decision in the pending appeal, there are no other such appeals, interferences, or related judicial proceedings.

A Related Proceedings Appendix is appended hereto.

- 5 -

**III STATUS OF CLAIMS (37 C.F.R. § 41.37(c) (1)(iii))**

RECEIVED  
CENTRAL FAX CENTER  
OCT 20 2006

**A. TOTAL NUMBER OF CLAIMS IN APPLICATION**

Claims in the application are: 1-27

**B. STATUS OF ALL THE CLAIMS IN APPLICATION**

1. Claims withdrawn from consideration: None
2. Claims pending: 1-27
3. Claims allowed: None
4. Claims rejected: 1-27
5. Claims cancelled: None

**C. CLAIMS ON APPEAL**

The claims on appeal are: 1-27

See additional status information in the Appendix of Claims.

OCT. 20. 2006 2:52PM

ZILKA-KOTAB, PC

NO. 4447 P. 11

- 6 -

RECEIVED  
CENTRAL FAX CENTER  
OCT 20 2006

**IV STATUS OF AMENDMENTS (37 C.F.R. § 41.37(c)(1)(iv))**

As to the status of any amendment filed subsequent to final rejection, there are no such amendments after final.

RECEIVED  
CENTRAL FAX CENTER  
OCT 20 2006

**V SUMMARY OF CLAIMED SUBJECT MATTER (37 C.F.R. § 41.37(e)(1)(v))**

With respect to a summary of Claim 1, as shown in Figures 1 and 3, computer program product for controlling operation of a computer to detect malware is provided. In use, pending scan database code is included for maintaining a pending scan database (e.g. see item 14 of Figure 1, etc.) storing data identifying computer files that have been written to a data storage device (e.g. see item 6 of Figure 1, etc.) and for which a scan for malware has yet to be performed. In addition, scanning code is included for conducting malware scanning (e.g. see item 44 of Figure 3, etc.) as a low priority task within a multitasking environment upon computer files identified within said pending scan database (e.g. see item 14 of Figure 1, etc.) as haven been written to the data storage device (e.g. see item 6 of Figure 1, etc.) and for which the scan for malware has yet to be performed. See, for example, page 5, line 21 – page 6; and page 7, lines 9-14 et al.

With respect to a summary of Claim 9, as shown in Figures 1 and 3, a method for detecting malware is provided. In use, a pending scan database is maintained (e.g. see item 14 of Figure 1, etc.) that stores data identifying computer files that have been written to a data storage device (e.g. see item 6 of Figure 1, etc.) and for which a scan for malware has yet to be performed. In addition, a malware scan is conducted (e.g. see item 44 of Figure 3, etc.) as a low priority task within a multitasking environment upon computer files identified within said pending scan database (e.g. see item 14 of Figure 1, etc.) as haven been written to the data storage device (e.g. see item 6 of Figure 1, etc.) and for which the scan for malware has yet to be performed. See, for example, page 5, line 21 – page 6; and page 7, lines 9-14 et al

With respect to a summary of Claim 17, as shown in Figures 1 and 3, an apparatus for detecting malware is provided. In use, pending scan database logic is included for maintaining a pending scan database (e.g. see item 14 of Figure 1, etc.) that stores data identifying computer files that have been written to a data storage device (e.g. see item 6 of Figure 1, etc.) and for which a scan for malware has yet to be performed. In addition, a scanner is included for conducting malware scanning (e.g. see item 44 of Figure 3, etc.) as a low priority task within a multitasking environment upon computer files identified within said pending scan database (e.g. see item 14 of Figure 1, etc.) as haven been written to the data storage device (e.g. see item 6 of Figure 1,

- 8 -

etc.) and for which the scan for malware has yet to be performed. See, for example, page 5, line 21 – page 6; and page 7, lines 9-14 et al

OCT. 20. 2006 2:52PM ZILKA-KOTAB, PC

NO. 4447 P. 14

- 9 -

RECEIVED  
CENTRAL FAX CENTER  
OCT 20 2006

**VI GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL (37 C.F.R. §  
41.37(c)(1)(vi))**

Following, under each issue listed, is a concise statement setting forth the corresponding ground of rejection.

**Issue # 1:** The Examiner has objected to Claims 1, 9, and 17 due to informalities.

**Issue # 2:** The Examiner has rejected Claims 1-27 under 35 U.S.C. 103(a) as being unpatentable over Cozza (U.S. Patent No. 5,502,815) in view of Waldin et al. (U.S. Patent No. 6,094,731).

- 10 -

**VII ARGUMENT (37 C.F.R. § 41.37(c)(1)(vii))**

RECEIVED  
CENTRAL FAX CENTER  
OCT 20 2006

The claims of the groups noted below do not stand or fall together. In the present section, appellant explains why the claims of each group are believed to be separately patentable.

**Issue # 1:**

The Examiner has objected to Claims 1, 9, and 17 due to informalities. Specifically, the Examiner has objected to appellant's claimed limitation of "have been written to a data storage device." Specifically, the Examiner has stated that such claim language should read "have not been written to a data storage device."

Appellant respectfully disagrees. In particular, appellant claims "a pending scan database storing data identifying computer files that have been written to a data storage device [but] for which a scan for malware has yet to be performed" and "conduct[ing] malware scanning upon [the] computer files identified within [the] pending scan database as haven been written to the data storage device [but] for which the scan for malware has yet to be performed" (see the same or similar, but not necessarily identical language in each of the independent claims-emphasis added).

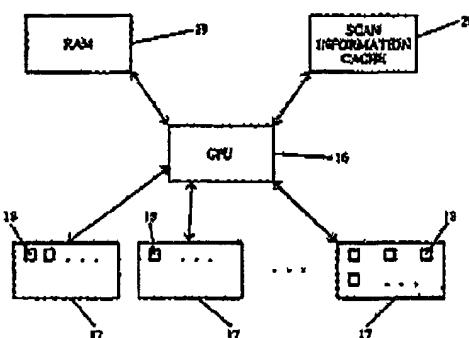
**Issue # 2:**

The Examiner has rejected Claims 1-27 under 35 U.S.C. 103(a) as being unpatentable over Cozza (U.S. Patent No. 5,502,815) in view of Waldin et al. (U.S. Patent No. 6,094,731).

***Group #1: Claims 1, 8-9, 16-17 and 24***

With respect to independent Claims 1, 9, and 17, the Examiner has relied on Figure 2 and Col. 3, lines 35-43 from Cozza, as cited below, to make a prior art showing of appellant's claimed "storing data identifying computer files that have been written to a data storage device and for which a scan for malware has yet to be performed."

- 11 -



(Cozza, Figure 2)

"Referring to FIG. 2, the apparatus for detecting computer viruses of the present invention includes a central processing unit 16. Information concerning the current state of volumes 17 or files 18 is stored in RAM 19, and information concerning prior states is stored in the scan information cache(s) 20. The cache 20 can be stored in any non-volatile storage medium including, but not limited to, the files or volumes being scanned." (Cozza, Col. 3, lines 35-42)

Appellant respectfully asserts that such excerpt relates to storing information on states of files such that changes in a fork size of the stored information may be utilized for determining a subset of viruses to scan for (see Abstract). Clearly, such excerpt does not even suggest appellant's claim language where "data [is stored that] identifies] computer files that have been written to a data storage device and for which a scan for malware has yet to be performed" (emphasis added), as claimed.

In the Office Action mailed 03/10/2006, the Examiner has responded to appellant's arguments by arguing that "Cozza explicitly discloses this information is stored in a cache in a non-volatile storage medium and when files are subsequently scanned for viruses (see Abstract)."

After a careful review of Cozza, appellant notes that the Abstract of Cozza discloses that the initial state information concerning the file "is stored in a cache in a non-volatile storage medium and when files are subsequently scanned for viruses, the current state information is compared to the initial state information stored in the cache" (emphasis added). Appellant also notes that when read in context, Cozza expressly discloses that the information stored in the cache particularly includes "information detailing the initial 'state' of an uninfected file or volume" (see Col. 2, lines 58-59). Thus, in Cozza, the information stored in the cache includes information on files that have already been scanned and determined to be uninfected. Appellant

- 12 -

on the other hand, claims "storing data identifying computer files that have been written to a data storage device and for which a scan for malware has yet to be performed" (emphasis added), as claimed. Clearly, storing the initial state information of a file in a cache, as in Cozza, fails to even suggest "storing data identifying computer files that have been written to a data storage device and for which a scan for malware has yet to be performed," as claimed by appellant.

Additionally, the Examiner has relied upon Col. 1, lines 20-45, Col. 3, lines 45-65 and Col. 6, lines 10-45 from Waldin to make a prior art showing of appellant's claimed "scanning code operable as a low priority task within a multitasking environment to conduct malware scanning upon computer files identified within said pending scan database as haven been written to the data storage device and for which the scan for malware has yet to be performed" (see the same or similar, but not identical language in each of the independent claims).

For substantially the same reasons as argued above, appellant respectfully asserts that neither Cozza nor Waldin teach "scanning code operable as a low priority task within a multitasking environment to conduct malware scanning upon computer files identified ... as haven been written to the data storage device and for which the scan for malware has yet to be performed," as claimed by appellant. Specifically, appellant asserts that the excerpts from Waldin relied upon by the Examiner simply fail to disclose "a low priority task" that operates on computer files identified "as haven been written to the data storage device and for which the scan for malware has yet to be performed" (emphasis added), as claimed by appellant.

In the Office Action mailed 03/10/2006, the Examiner has responded to appellant's arguments by arguing that "this argument does not make sense because Appellant did not claim this limitation 'as haven been written to a data storage device and for which a scan for malware has yet to be performed' as discussed in the previous Office action."

Appellant respectfully asserts that each of the independent claims specifically require "conduct malware scanning upon computer files identified within said pending scan database as haven been written to the data storage device and for which the scan for malware has yet to be performed" [see the same or similar, but not necessarily identical language in part (ii) of each of the independent claims].

- 13 -

Thus, appellant respectfully asserts that the excerpts in Waldin relied on by the Examiner only disclose "a cache of files that have been scanned and certified clean" (Col. 1, lines 26-27), "[o]nce a file is scanned, a hash value (or simply 'hash') of the contents of the file is stored in a database" (Col. 1, lines 40-41), an "[a]ntivirus scan module" (Col. 3, line 56), and "rescan[ning] the entire file" if modules at a recipient computer and a originating computer are not identical (Col. 6, lines 10-36). Clearly, Waldin merely teaches scanning at an originating computer and then again at a recipient computer for comparing hashes generated by each scan (see Abstract), which does not even suggest "conduct[ing] malware scanning upon computer files identified within said pending scan database as haven been written to the data storage device and for which the scan for malware has yet to be performed" (see the same or similar, but not necessarily identical language in each of the independent claims-emphasis added).

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on appellant's disclosure. *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed.Cir.1991).

Appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above.

*Group #2: Claims 2, 10, and 18*

With respect to Claims 2, 10, and 18, the Examiner has relied on Col. 2, line 55-Col. 3, line 8 from Cozza, as cited below, to make a prior art showing of appellant's claimed technique where "file write code [that is] operable as a computer file is written to a storage device to add data identifying said computer file to said pending scan database."

- 14 -

"The method and apparatus of the present invention for scanning files for computer viruses relies on the fact that viruses invariably change the file or volume they infect. Consequently, information detailing the initial "state" of an uninfected file or volume can be "cached" or securely saved to disk or other non-volatile storage medium. The cached information is dependent not only on the type of machine the scanning program is running on, but also on viruses' method of infection on that type of machine. The stored information can be tailored to meet the variety of situations found in present and future computing environments.

Once the initial "state" information has been stored to a disk or other non-volatile storage medium, the method and apparatus of the present invention can use this cached information in future virus scans to determine what files and/or volumes have changed in a way indicative of most virus infections. In many applications this information alone is enough to eliminate the need to scan a file/volume for most, if not all, viruses. The result is a substantial improvement in scanning time, in return for a very modest cost in terms of disk or other non-volatile storage medium." (Cozza, Col. 2, line 55 - Col. 3, line 6)

Appellant respectfully asserts that such excerpt only teaches that "information detailing the initial 'state' of an uninfected file...can be 'cached'." However, Cozza does not teach when such state information is stored, but only that the file must be in an initial state. Clearly, only generally teaching storing initial state information of a file, as in Cozza, does not meet appellant's specific claim language, namely that "as a computer file is written to a storage device...data identifying said computer file [is added] to said pending scan database" (emphasis added). Furthermore, Cozza only teaches that the state information is stored, but not that it is stored to a "pending scan database," as claimed by appellant. In fact, Cozza only scans a current state data, which would not require the initial state information to be stored in a pending scan database.

Again, appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above.

*Group #3: Claims 3, 11, and 19*

With respect to Claims 3, 11, and 19, the Examiner has relied on Col. 3, lines 45-55 from Cozza, as cited below, to make a prior art showing of appellant's claimed "file read code [that is]

- 15 -

operable in response to a read request for a computer file included within said pending scan database to trigger said scanning code to scan said computer file as a high priority task before permitting read access to said computer file."

"In this process, which while described with reference to a Macintosh computer may be used with virtually any other computer, each volume 17 with its files or any subset thereof stored in a memory system is scanned. Before commencing the actual scan, however, the volume being scanned is examined for the scan information cache (which, in a preferred embodiment, is a file) in step 24 which is located at a predetermined place on the volume being scanned or on some other accessible volume. If the file is found, it is read into RAM or some other high speed memory in step 26, and its contents are verified in step 28." (Cozza, Col. 3, lines 45-55 - emphasis added)

Appellant respectfully asserts that the excerpt from Cozza relied upon by the Examiner merely discloses that "[b]efore commencing the actual scan ... the volume being scanned is examined for the scan information cache" and "[i]f the file is found, it is read into RAM or some other high speed memory in step 26, and its contents are verified in step 28." However, the mere disclosure of reading a scan information cache into RAM before commencing a scan, as in Cozza, fails to even suggest a situation of "a read request for a computer file," as appellant claims. Thus, Cozza fails to teach appellant's specifically claimed "file read code [that is] operable in response to a read request for a computer file included within said pending scan database to trigger said scanning code to scan said computer file as a high priority task before permitting read access to said computer file" (emphasis added), as claimed by appellant.

Again, appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above.

*Group #4: Claims 4-6, 12-14, and 20-22*

With respect to Claims 4, 12, and 20, the Examiner has relied on Col. 3, lines 35-40 in Cozza, as cited below, to make a prior art showing of appellant's claimed "scanned file database code [that is] operable to maintain a scanned file database storing data identifying computer files that have been scanned for malware."

- 16 -

"Referring to FIG. 2, the apparatus for detecting computer viruses of the present invention includes a central processing unit 16. Information concerning the current state of volumes 17 or files 18 is stored in RAM 19, and information concerning prior states is stored in the scan information cache(s) 20. The cache 20 can be stored in any non-volatile storage medium including, but not limited to, the files or volumes being scanned." (Cozza, Col. 3, lines 35-42)

Appellant respectfully asserts that such excerpt only teaches storing information on a current state and prior states of a file. When read in context, Cozza stores such states for determining what set of viruses to scan the associated file for (see Abstract). Thus, Cozza does not teach a "scanned file database...[for] storing data identifying computer files that have been scanned for malware" (emphasis added), as claimed.

Again, appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above.

*Group #5: Claims 7, 15, and 23*

With respect to Claims 7, 15, and 23, the Examiner has relied on Col. 3, lines 35-55 in Cozza, as cited below, to make a prior art showing of appellant's claimed "initiation code [that is] operable upon startup to detect any computer files stored on a storage device not included within either said pending scan database or said scanned file database and to add such computer files to said pending scan database."

"Referring to FIG. 2, the apparatus for detecting computer viruses of the present invention includes a central processing unit 16. Information concerning the current state of volumes 17 or files 18 is stored in RAM 19, and information concerning prior states is stored in the scan information cache(s) 20. The cache 20 can be stored in any non-volatile storage medium including, but not limited to, the files or volumes being scanned.

Referring now to FIG. 3, the process for scanning for computer viruses of the present invention will now be described. In this process, which while described with reference to a Macintosh computer may be used with virtually any other computer, each volume 17 with its files or any subset thereof stored in a memory system is scanned. Before commencing the actual scan, however, the volume being scanned is examined for the scan information cache (which, in a preferred embodiment, is a file) in step 24 which is located at a predetermined place on the volume being

- 17 -

scanned or on some other accessible volume. If the file is found, it is read into RAM or some other high speed memory in step 26, and its contents are verified in step 28." (Cozza, Col. 3, lines 35-55)

Appellant respectfully asserts that Cozza only teaches storing states of files and using such states to scan each file "stored in a memory system." However, Cozza does not specifically teach a "pending scan database" and "scanned file database," let alone detecting "upon startup... any computer files stored on a storage device not included within either said pending scan database or said scanned file database and...add[ing] such computer files to said pending scan database" (emphasis added), as claimed by appellant.

Again, appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above.

*Group #6: Claim 25*

With respect to Claim 25, the Examiner has relied on Col. 3, lines 50-67 and Col. 4, lines 15-60 in Cozza to make a prior art showing of appellant's claimed technique "wherein an order of said computer files identified within said pending scan database being scanned is based on an algorithm that estimates the likelihood of a read request being performed on each computer file."

Appellant respectfully asserts that the excerpts from Cozza relied upon by the Examiner disclose that "[f]or each file on a volume that is to be scanned, the cache is searched for the presence of the file's cache information in step 40." However, merely searching for the file's cache information, as in Cozza, simply fails to even suggest any "order of said computer files identified within said pending scan database," as claimed by appellant. Furthermore, the excerpts from Cozza fail to disclose that the ordering is "based on an algorithm that estimates the likelihood of a read request being performed on each computer file," as specifically claimed by appellant.

Again, appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above.

- 18 -

*Group #7: Claim 27*

With respect to Claim 27, the Examiner has relied on Col. 3, lines 50-67 and Col. 4, lines 15-60 in Cozza to make a prior art showing of appellant's claimed technique "wherein an order of said computer files identified within said pending scan database being scanned is based on the order in which said computer files were placed in said pending scan database."

Appellant respectfully asserts that the excerpts from Cozza relied upon by the Examiner disclose that "[f]or each file on a volume that is to be scanned, the cache is searched for the presence of the file's cache information in step 40." However, merely searching for the file's cache information, as in Cozza, simply fails to even suggest any "order of said computer files identified within said pending scan database," as claimed by appellant. Furthermore, the excerpts from Cozza fail to disclose that the ordering is "based on the order in which said computer files were placed in said pending scan database," as specifically claimed by appellant.

Again, appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above.

*Group #8: Claim 26*

With respect to Claim 26, the Examiner has relied on Col. 4, line 59 to Col. 5, line 7 in Cozza, as cited below, to make a prior art showing to appellant's claimed technique "wherein only computer files determined to be clean from the malware scanning are stored in the scanned file database."

"After all virus scanning for a file is completed, the scan cache must be updated. It is preferable to keep a second, new cache in memory separate from the original cache and update that with the new information for each file on the disk (thus eliminating outdated information in the old cache). To update the cache, the scan results are checked to determine whether any virus was found in step 58. If a virus was found, then the scan cache is updated with zeroed information for the file in step 60, which will force the file to be completely scanned again in the future. If no viruses were found in the file, then the file's scan information is added to the new cache in step 62. This information includes the file's ID, resource fork length and data fork

- 19 -

length. Steps 38 through 64 are repeated for each scannable file on the disk. When all files have been scanned on the volume, the new, updated cache is written to disk on the volume scanned (34)." (Cozza, Col. 4, line 59 - Col. 5, line 7)

Appellant respectfully asserts that the excerpts from Cozza relied upon by the Examiner disclose that "[i]f a virus was found, then the scan cache is updated with zeroed information for the file in step 60" (emphasis added). However, updating the scan cache with zeroed information for a file found to have a virus *teaches away* from a technique "wherein only computer files determined to be clean from the malware scanning are stored in the scanned file database" (emphasis added), as claimed by appellant.

Again, appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above.

In view of the remarks set forth hereinabove, all of the independent claims are deemed allowable, along with any claims depending therefrom.

- 20 -

RECEIVED  
CENTRAL FAX CENTER**VIII CLAIMS APPENDIX (37 C.F.R. § 41.37(c)(1)(viii))****OCT 20 2006**

The text of the claims involved in the appeal (along with associated status information) is set forth below:

1. (Previously Presented) A computer program product for controlling operation of a computer to detect malware, said computer program product comprising:
  - (i) pending scan database code operable to maintain a pending scan database storing data identifying computer files that have been written to a data storage device and for which a scan for malware has yet to be performed; and
  - (ii) scanning code operable as a low priority task within a multitasking environment to conduct malware scanning upon computer files identified within said pending scan database as having been written to the data storage device and for which the scan for malware has yet to be performed.
2. (Previously Presented) A computer program product as claimed in claim 1, further comprising file write code operable as a computer file is written to a storage device to add data identifying said computer file to said pending scan database.
3. (Original) A computer program product as claimed in claim 1, further comprising file read code operable in response to a read request for a computer file included within said pending scan database to trigger said scanning code to scan said computer file as a high priority task before permitting read access to said computer file.
4. (Original) A computer program product as claimed in claim 1, further comprising scanned file database code operable to maintain a scanned file database storing data identifying computer files that have been scanned for malware.
5. (Original) A computer program product as claimed in claim 4, wherein said data identifying computer files that have been scanned for malware includes checksum data derived from said computer files that were scanned.

- 21 -

6. (Original) A computer program product as claimed in claim 5, further comprising file read code operable in response to a read request for a computer file to detect if said computer file is within said scanned file database and a checksum value recalculated for said computer file matches that stored within said scanned file database before permitting said read request.
7. (Original) A computer program product as claimed in claim 4, further comprising initiation code operable upon startup to detect any computer files stored on a storage device not included within either said pending scan database or said scanned file database and to add such computer files to said pending scan database.
8. (Original) A computer program product as claimed in claim 1, wherein said malware comprises one or more of:
  - (i) a computer file infected with a computer virus;
  - (ii) a Trojan;
  - (iii) a banned computer file; and
  - (iv) a computer file containing banned content.
9. (Previously Presented) A method for detecting malware, said method comprising the steps of:
  - (i) maintaining a pending scan database storing data identifying computer files that have been written to a data storage device and for which a scan for malware has yet to be performed; and
  - (ii) as a low priority task within a multitasking environment, conducting malware scanning upon computer files identified within said pending scan database as having been written to the data storage device and for which the scan for malware has yet to be performed.
10. (Original) A method as claimed in claim 9, further comprising the step of as a computer file is written to a storage device adding data identifying said computer file to said pending scan database.

- 22 -

11. (Original) A method as claimed in claim 9, further comprising the step of in response to a read request for a computer file included within said pending scan database, triggering scanning of said computer file as a high priority task before permitting read access to said computer file.
12. (Original) A method as claimed in claim 9, further comprising maintaining a scanned file database storing data identifying computer files that have been scanned for malware.
13. (Original) A method as claimed in claim 12, wherein said data identifying computer files that have been scanned for malware includes checksum data derived from said computer files that were scanned.
14. (Original) A method as claimed in claim 13, further comprising the step of in response to a read request for a computer file, detecting if said computer file is within said scanned file database and a checksum value recalculated for said computer file matches that stored within said scanned file database before permitting said read request.
15. (Original) A method as claimed in claim 12, further comprising the step of upon startup detecting any computer files stored on a storage device not included within either said pending scan database or said scanned file database and to add such computer files to said pending scan database.
16. (Original) A method as claimed in claim 9, wherein said malware comprises one or more of:
  - (i) a computer file infected with a computer virus;
  - (ii) a Trojan;
  - (iii) a banned computer file; and
  - (iv) a computer file containing banned content.
17. (Previously Presented) Apparatus for detecting malware, said apparatus comprising:
  - (i) pending scan database logic operable to maintain a pending scan database storing data identifying computer files that have been written to a data storage device and for which a scan for malware has yet to be performed; and

- 23 -

(ii) a scanner operable as a low priority task within a multitasking environment to conduct malware scanning upon computer files identified within said pending scan database as haven been written to the data storage device and for which the scan for malware has yet to be performed.

18. (Original) Apparatus as claimed in claim 17, further comprising file write logic operable as a computer file is written to a storage device to add data identifying said computer file to said pending scan database.

19. (Original) Apparatus as claimed in claim 17, further comprising file read logic operable in response to a read request for a computer file included within said pending scan database to trigger said scanning logic to scan said computer file as a high priority task before permitting read access to said computer file.

20. (Original) Apparatus as claimed in claim 17, further comprising scanned file database logic operable to maintain a scanned file database storing data identifying computer files that have been scanned for malware.

21. (Original) Apparatus as claimed in claim 20, wherein said data identifying computer files that have been scanned for malware includes checksum data derived from said computer files that were scanned.

22. (Original) Apparatus as claimed in claim 21, further comprising file read logic operable in response to a read request for a computer file to detect if said computer file is within said scanned file database and a checksum value recalculated for said computer file matches that stored within said scanned file database before permitting said read request.

23. (Original) Apparatus as claimed in claim 20, further comprising initiation logic operable upon startup to detect any computer files stored on a storage device not included within either said pending scan database or said scanned file database and to add such computer files to said pending scan database.

- 24 -

24. (Original) Apparatus as claimed in claim 17, wherein said malware comprises one or more of:

- (i) a computer file infected with a computer virus;
- (ii) a Trojan;
- (iii) a banned computer file; and
- (iv) a computer file containing banned content.

25. (Previously Presented) A computer program product as claimed in claim 1, wherein an order of said computer files identified within said pending scan database being scanned is based on an algorithm that estimates the likelihood of a read request being performed on each computer file.

26. (Previously Presented) A computer program product as claimed in claim 4, wherein only computer files determined to be clean from the malware scanning are stored in the scanned file database.

27. (Previously Presented) A computer program product as claimed in claim 1, wherein an order of said computer files identified within said pending scan database being scanned is based on the order in which said computer files were placed in said pending scan database.

OCT. 20. 2006 2:57PM ZILKA-KOTAB, PC

NO. 4447 P. 30

- 25 -

**IX EVIDENCE APPENDIX (37 C.F.R. § 41.37(c)(1)(ix))**

RECEIVED  
CENTRAL FAX CENTER

OCT 20 2006

There is no such evidence.

OCT. 20. 2006 2:57PM ZILKA-KOTAB, PC

NO. 4447 P. 31

- 26 -

**X RELATED PROCEEDING APPENDIX (37 C.F.R. § 41.37(c)(1)(x))**

There is no such related proceeding.

RECEIVED  
CENTRAL FAX CENTER  
OCT 20 2006

- 27 -

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 971-2573. For payment of any additional fees due in connection with the filing of this paper, the Commissioner is authorized to charge such fees to Deposit Account No. 50-1351 (Order No. NAI1P486/01.060.01).

Respectfully submitted,

By: \_\_\_\_\_

Kevin J. Zilka

Reg. No. 41,429

Date: 10/20/06

Zilka-Kotab, P.C.  
P.O. Box 721120  
San Jose, California 95172-1120  
Telephone: (408) 971-2573  
Facsimile: (408) 971-4660